IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims

1. – 9. (Cancelled)

10. (Currently amended) A method for detecting the presence of a computer virus, the method comprising;

receiving, at a bait server, a request for access to ~~perform a function on~~ the bait server, wherein the bait server's address is not published to a network and wherein receipt of the request indicates that a virus attack is in progress;

identifying an offending system from which the request originated;

alerting a local server that [[a]] the virus attack is in progress and of the identity of the offending system; and

disconnecting the offending system from the network.

11. (Original) The method as recited in claim 10, further comprising:

prior to disconnecting the offending system, notifying the offending system that it is infected with a virus.

12. (Original) The method as recited in claim 10, further comprising:

receiving a reconnect request from the offending system;

verifying that the offending system is disinfected and available to reconnect to the network; and

reconnecting the offending system to the network.

13. (Cancelled)

14. (Cancelled)

15. (Cancelled)

16. (Currently amended) A method in a bait server for detecting the presence of a computer virus, the method comprising:

not publishing the bait server's address to a network;

receiving a request for access from the network, wherein receipt of the request indicates that a virus is present;

~~monitoring the network for the presence of a computer virus;~~

~~responsive to a determination that a virus is detected,~~ determining the identity of an offending system within the network from which the virus entered the network;

notifying a local server of the presence of the virus and the identity of the offending system;

instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication;

directing the local server to disconnect the offending system from the network; and

responsive to an indication that the offending system has been disinfected and responsive to a reconnect request from the offending system to the local server, reconnecting the offending system to the network.

17. (Previously presented) The method as recited in claim 10, further comprising:

instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication.

18. (Cancelled)

19. (Cancelled)

20. (Currently amended) A computer program product in a computer readable media for use in a data processing system for detecting the presence of a computer virus, the computer program product comprising;

first instructions for receiving, at a bait server, a request for access to ~~perform a function on~~ the bait server, wherein the bait server's address is not published to a network and wherein receipt of the request indicates that a virus attack is in progress;

second instructions for identifying an offending system from which the request originated;

third instructions for alerting a local server that [[a]] the virus attack is in progress and the identity of the offending system; and

fourth instructions for disconnecting the offending system from [[a]] the network.

21. (Original) The computer program product as recited in claim 20, further comprising:

fifth instructions for, prior to disconnecting the offending system, notifying the offending system that it is infected with a virus.

22. (Original) The computer program product as recited in claim 20, further comprising:

fifth instructions for receiving a reconnect request from the offending system;

sixth instructions for verifying that the offending system is disinfected and available to reconnect to the network; and

seventh instructions for reconnecting the offending system to the network.

23. (Cancelled)

24. (Cancelled)

25. (Cancelled)

26. (Currently amended) A computer program product in a computer readable media for use in a data processing system in a bait server for detecting the presence of a computer virus, the computer program product comprising:

first instructions for not publishing the bait server's address published to a network;

second instructions for ~~monitoring the network for the presence of a computer virus;~~ receiving a request for access from the network, wherein receipt of the request indicates that a virus is present;

third instructions~~, responsive to a determination that a virus is detected,~~ for determining the identity of an offending system within the network from which the virus entered the network;

fourth instructions for notifying a local server of the presence of the virus and the identity of the offending system;

fifth instructions for instructing all devices within the network to ignore all requests from the offending system until the offending system is reauthorized for network communication;

sixth instructions for directing a local server to disconnect the offending system from the network; and

seventh instructions, responsive to an indication that the offending system has been disinfected and responsive to a reconnect request from the offending system to the local server, for reconnecting the offending system to the network.

27. (Previously presented) The computer program product as recited in claim 20, further comprising:

fifth instructions for instructing all devices within the network to ignore all requests from the offending system until the offending system is reauthorized for network communication.

28. (Cancelled)

29. (Cancelled)

30. (Currently amended) A system for detecting the presence of a computer virus, the system comprising;

a receiver, at a bait server, which receives a request for access to ~~perform a function on~~ the bait server, wherein the bait server's address is not published to a network and wherein receipt of the request indicates that a virus attack is in progress;

an identifying unit which identifies an offending system from which the request originated;

[~~an~~] a virus alert unit which alerts a local server that [[a]] the virus attack is in progress and the identity of the offending system; and

a disconnection unit which disconnects the offending system from [[a]] the network.

31. (Original) The system as recited in claim 30, further comprising:

a notification unit which, prior to disconnecting the offending system, notifies the offending system that it is infected with a virus.

32. (Original) The system as recited in claim 30, further comprising:

a reconnect request unit which receives a reconnect request from the offending system;

a verification unit which verifies that the offending system is authorized to reconnect to the network; and

a reconnecting unit which reconnects the offending system to the network.

33. (Cancelled)

34. (Cancelled)

35. (Cancelled)

36. (Currently amended) A system in a bait server for detecting the presence of a computer virus, the system comprising:

a ~~monitoring~~ receiving unit which receives a request for access from a network, ~~monitors a network for the presence of a computer virus,~~ wherein the bait server's address is not published to the network and wherein receipt of the request indicates that a virus is present;

an identifier unit which~~, responsive to a determination that a virus is detected,~~ determines the identity of an offending system within the network from which the virus entered the network;

a notification unit which notifies a local server of the presence of the virus and the identity of the offending system;

a network protection unit which instructs all devices within the network to ignore all requests from the offending system until the offending system is reauthorized for network communication; [[~~and~~]]

a disconnection unit which directs a local server to disconnect the offending system from the network[[~~.~~]]; and

a reconnection unit which, responsive to an indication that the offending system has been disinfected and responsive to a reconnect request from the offending system to the local server, reconnects the offending system to the network.

37. (Previously presented) The system as recited in claim 30, further comprising:

a network protection unit which instructs all devices within the network to ignore all requests from the offending system until the offending system is reauthorized for network communication.

38. (Cancelled)

39. (Cancelled)